REMARKS/ARGUMENTS

Applicant submits this response to the Office Action dated August 26, 2004. Applicant has amended claims 1-4, cancelled claim 16 and added new claims 19-26. Claims 1-4 and 19-26 remain pending. No new matter has been added.

In the Office Action, the Examiner has rejected claims 1-4 and 16 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,643,287 to Callon et al. ("Callon"). As Applicant has cancelled claim 16, the rejection of this claim is moot. Applicant respectfully requests that the Examiner reconsider the remaining rejections based upon the following.

Callon describes a system that allows for packets from distributed private networks to be transmitted to each other across a public Internet. (Callon, col. 6, ll. 27-36.) Callon describes a private network X that is distributed over two sites X' and X'' which are connected to a public IP network at nodes A and F, respectively. (Id., col. 6, ll. 37-41, Fig. 3.) The router at node A encapsulates packets from the private network at X' within an IP packet for transmission over the public network, while the router at node F de-encapsulates those packets and transmits them over the private network at location X''. (Id., col. 6, ll. 41-48.) In one specific example, Callon describes a situation where a "private Ethernet packet" is encapsulated by a router adding a "public ISP IP header to the packet ... to generate an encapsulated packet ... for transmission over the IP network." (Id., col. 7, ll. 35-42.) The public ISP IP header includes a source IP address that "specif[ies] the X' private network at node A," and a destination IP address that "specif[ies] the X'' private network at node F." (Id., col. 6, ll. 52-57.)

Callon notes that when a packet is received at an "ingress node," a hash function is typically performed on the source and destination addresses of the packet (as well as the protocol field and the TCP port field, if any) in order to determine the path by which to route the packet over the public network to the "egress router." (Id., col. 3, ll. 19-28.) Callon states that this may be a problem for encapsulated packets sent between portions of a private network, as since the source and destination addresses are the same for every packet (the ingress and egress routers addresses), the hash function will generate the same path for every packet, which may overload the path. (Id., col. 3, l. 63 to col. 4, l. 18.) As a solution to this stated problem, Callon further describes a system and method that performs a hash on both the public IP header (the encapsulating header) and the private IP header or other information "which uniquely identify

source and destination nodes in the private network." (Id., col. 8, ll. 6-29.) The hash produces a value that is inserted into a "low-order portion" of the source IP address used to encapsulate the packet. (Id., col. 9, ll. 6-12.) When other routers in the public network perform the hash on the encapsulating header, the value causes the hash to vary depending on the private network source and destination nodes, and effectively distributes the traffic over multiple paths in the public network. (Id., col. 8, ll. 33-39.)

In contrast to the description in Callon, claim 1 recites a method that includes:

> a) receiving a packet having a layer 2 destination address and a first layer 3 destination address at a receiving port;
>
> b) modifying the packet by replacing the layer 2 destination address with context information based on the receiving port;
>
> c) determining a second layer 3 destination address based on at least a portion of the first layer 3 destination address; and
>
> d) encapsulating the modified packet with the second layer 3 destination address.

Callon does not describe such a method. For example, Callon does not describe modifying a packet by replacing a layer 2 destination address with context information based on the port at which the packet was received. Callon merely describes encapsulating a private network packet with an IP (layer 3) header having source and destination IP addresses, and varying the encapsulating source IP address by hashing on network information in the packet. Such description does not teach or suggest (at least) "modifying the packet by replacing the layer 2 destination address with context information based on the receiving port" as recited by claim 1. As Callon does not include all of the elements of claim 1, it cannot anticipate claim 1, and Applicant respectfully requests that the Examiner withdraw the rejection of this claim. As claims 2 and 3 depend from claim 1, and therefore include all of the limitations of claim 1, Applicant believes claims 2 and 3 to be patentable over Callon at least for the same reasons as claim 1, and therefore respectfully requests that the Examiner withdraw the rejections of claims 2 and 3 as well.

Likewise, claim 4 recites a method comprising:

> a) receiving an encapsulated packet having context information, a first layer 3 destination address, and a second layer 3 destination address, the context information indicating a first network;

b) creating a de-encapsulated packet by removing the second layer 3 destination address from the encapsulated packet;

c) determining a destination layer 2 address based on (i) at least a portion of the first layer 3 destination address, and (ii) at least a portion of the context information;

d) replacing the context information with the determined destination layer 2 address in the de-encapsulated packet; and

(e) sending the packet to a second network;

wherein the first network and second network share a layer 2 address space containing the determined destination layer 2 address.

Callon does not describe such a method. For example, Callon does not describe replacing context information in a de-encapsulated packet with a destination layer 2 address. As noted above, Callon merely describes encapsulating a private network packet with an IP (layer 3) header having source and destination IP addresses, and varying the encapsulating source IP address by hashing on network information in the packet. Such description does not teach or suggest (at least) "replacing the context information with the determined destination layer 2 address in the de-encapsulated packet" as recited by claim 4. As Callon does not include all of the elements of claim 4, it cannot anticipate claim 4, and Applicant respectfully requests that the Examiner withdraw the rejection of this claim.

Applicant has added new claims 19-26. Claims 19-20 are dependent on claim 1, and therefore include all of the limitations of claim 1. As a result, Applicant believes claims 19 and 20 to be patentable at least based on the reasons discussed for claim 1. Claims 21-24 are dependent on claim 4, and therefore include all of the limitations of that claim. As a result, Applicant believes claims 21-24 to be patentable at least for the reasons discussed for claim 4. Claims 25 and 26 are independent claims that further define the scope of the invention disclosed and supported by the embodiments described in the present application, and Applicant believes these claims to be patentable over Callon.

In view of the foregoing amendments and remarks, Applicant respectfully submits that the pending claims are in condition for allowance. Accordingly, Applicant requests that the Examiner pass this application to issue. If there are any outstanding issues which need to be resolved to place the application in condition for allowance, the Examiner is invited to contact Applicant's undersigned representative by phone to discuss and hopefully resolve such issues.

Respectfully submitted,

Date: October 8, 2004

Joseph R. Palmieri
Reg. No. 40,760

Verizon Corporate Services Group Inc.
600 Hidden Ridge Drive
Mail Code: HQE03H14
Irving, Texas 75038
(972) 718-4800